AD-A249 878

92-12854

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release. Distribution is unlimited.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION U.S. Army War College 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) Root Hall, Building 122 Carlisle, PA 17013	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)

Intelligence Support to Low-Intensity Conflicts

12. PERSONAL AUTHOR(S)
LTC Talmadge R. Varnado

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Individual Study	FROM _____ TO _____	1992 April 15	43

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The global reach of the U.S. intelligence system will play a greater role in responding to international challenges to U.S. interests. This phenomenon will bring about a new intelligence era with new tasks and new priorities. This is particularly true when a low-intensity conflict (LIC) is viewed as the most probable conflict requiring the commitment of military instruments--security assistance, communications, civic action, psychological operations, medical, logistical, and intelligence support. Major changes are required in current doctrine and organization to enhance the effectiveness of intelligence support to LIC operations. If the military intelligence community is to join the intelligence "burden sharing" alliance, it must be driven by the five LIC imperatives, observe the ten principles of intelligence support to LIC, exercise LIC scenarios in a BCTP type environment, and incorporate a dynamic IEW architecture capable of accommodating complementary, rather than redundant, analysis.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION	
☐ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL Mr. Douglas Dearth	22b. TELEPHONE (Include Area Code) (717) 245-3191	22c. OFFICE SYMBOL AWCAC

DD Form 1473, JUN 86 *Previous editions are obsolete.* SECURITY CLASSIFICATION OF THIS PAGE

USAWC Military Studies Program Paper

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

Intelligence Support to Low-Intensity Conflicts

An Individual Study Project

by

LTC Talmadge R Varnado, II
United States Army

Mr. Doug Dearth
Project Adviser

Accesion For
NTIS CRA&I
DTIC TAB
Unannounced
Justification
By
Distribution /
Availability Codes
Dist | Avail and / or Special
A-1

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

Abstract

Author: Talmadge R. Varnado, II, LTC, USA

Title: Intelligence Support to Low-Intensity Conflicts

Format: Individual Study Project

Date: 15 April 1992 Pages: 43 Classification: Unclassified

The global reach of the U.S. intelligence system will play a greater role in responding to international challenges to U.S. interests. This phenomenon will bring about a new intelligence era with new tasks and new priorities. This is particularly true when low-intensity conflict (LIC) is viewed as the most probable conflict requiring the commitment of military instruments—security assistance, communications, civic action, psychological operations, medical, logistical, and intelligence support. Major changes are required in current doctrine and organization to enhance the effectiveness of intelligence support to LIC operations. If the military intelligence community is to join the intelligence "burden sharing" alliance, it must be driven by the five LIC imperatives, observe the ten principles of intelligence support to LIC, exercise LIC scenarios in a BCTP type environment, and incorporate a dynamic IEW architecture capable of accommodating complementary, rather than redundant, analysis.

Table of Contents

	Page
Introduction	1
Five Imperatives	4
Ten Principles of Intelligence Support to LIC	6
Intelligence Capability Spectrum	9
Shedding the Conventional Mindset	13
The IEW Synchronization Matrix in LIC	17
Intelligence Data Bases	21
Intelligence: The Common Thread in All LIC Operations	23
Battle Command Training Program (BCTP) for LIC	27
A Different Approach	29
A Feasible IEW Architecture	31
Conclusion	38
Notes	40
Bibliography	42

Table of Illustrations

		Page
Figure 1.	Intelligence Capability Spectrum Matrix (SIGINT)	10
Figure 2.	Intelligence Capability Spectrum Matrix (IMINT)	11
Figure 3.	Intelligence Capability Spectrum Matrix (HUMINT)	12
Figure 4.	Mindset Transfer Matrix	16
Figure 5.	The 1st Cavalry Division IEW Synchronization Matrix ("Razor's Edge")	19
Figure 6.	IEW Synchronization Matrix in LIC	20
Figure 7.	IEW Architecture	34
Figure 8.	IEW Architecture	35
Figure 9.	IEW Architecture (ELINT)	36
Figure 10.	IEW Architecture (COMINT)	36
Figure 11.	IEW Architecture (Digitized Imagery)	37
Figure 12.	IEW Architecture HUMINT)	37

Introduction

In the aftermath of the collapse of the Warsaw Pact and the dissolution of the Soviet Union, strategic uncertainty for American decision-makers and military planners has increased. While strategic global conflict has become far less likely, future national security threats probable will be more regional in nature. Within this context, low intensity conflict (LIC) will become the most probable environment for the commitment of the U.S. Army forces.

As stated in the National Security Strategy of the United States, August 1991:

> "The unprecedented scope and pace of change in today's world—and the increasing number of actors now able to threaten global peace—highlight the need for reliable information and a sophisticated understanding of events and trends. The global reach of American intelligence capabilities is a unique national asset, crucial not only to our own security, but also to our leadership role in responding to international challenges."[1]

The most significant threat to U.S. interests in LIC is not found in the individual cases of insurgency, economic instability, narcotics trafficking or in isolated acts of terrorism and subversion.[2] Rather, it results from the synergistic and cumulative effects from such activities. Such outcomes can gradually isolate the United States, its allies and global trading partners from the Third World and from one another.[3]

Long term separation could have an impact on the access to strategic minerals and energy sources.[4] A residual effect could be the crumbling of democracy and loss of human rights precipitating an uncontrolled large-scale migration.[5] The U.S. could lose critical military bases, transit, and access rights. The cumulative effects of such isolation could precipitate the gradual shifting of friends and allies into positions of accommodation with interests hostile to the United States.[6]

Combating the potential threat to U.S. interest in a LIC environment requires a balanced and integrated application of the political, economic, informational, and military instruments of U.S. national power.[7] The military instruments are non-combat military measures, such as security assistance, intelligence, communications, civic action, psychological operations, engineering, medical and logistical support.[8] "LIC is a psychological war with political and security aspects fought to achieve social, political, economic and psychological goals."[9]

Success in LIC depends upon having a strategy which is comprehensive and integrated with regional policies to ensure that the instruments of national power are coordinated and balanced. The strategy must clearly define the U.S. Government's role and interagency responsibilities, with the Department of Defense (DoD) in a principally supporting role for overall U.S. Government policy. At the same time DoD must provide the force structure and resources capable of effectively supporting Administration policy.[10]

The purpose of this paper is not to try to develop a procedure that will automatically insure a consensus among all the LIC players—Department of State, Department of Defense, Central Intelligence Agency, Military Services, host nations, etc. Nor is it to reorganize the national -level intelligence structure or to complain about force structure and budget reductions. The assumption will be made that the problems existing in these areas will be resolved in the best interest of the nation. The purpose of this paper is to offer suggestions on how military intelligence can better satisfy the intelligence support requirements generated by the complex environment of LIC.

The person experiencing the greatest sense of inadequacy in the world today is a nineteen year old intelligence analyst assigned to a corps or division who no longer has the mission to "locate, identify and kill Russians." He has committed every available Soviet doctrinal template to memory. He can identify every vehicle in a combined arms army. He knows the capability of every Soviet air defense system. He has mastered the

five functions of the intelligence preparation of the battlefield (IPB) process. And now, he has been told there is no more Soviet threat and that LIC, a psychological war fought to achieve social, political, economic and psychological goals, is the most probable form of engagement the U.S. Army will be involved. This young analyst is the linchpin to the intelligence system and whom we must convince early on that the intelligence support to LIC is more challenging and plays an important role in the formulation of national policy.

A mindset transfer from conventional war to LIC must take place in order for the U.S. Army to be effective in a LIC supporting role, not only with the young analyst but with the entire army (to include mid-level and senior leadership). This paper will outline some imperatives, principles and insights on how to shed the conventional mindset.

The complexities of LIC can be understood by investigating the composition of some of the types of information that the economic, social, political, geographical and military data bases should contain. The scope of the paper is tailored to risk and security challenges.

The following discussion is intended to demonstrate why intelligence is vital to all the LIC components and what is involved in providing quality intelligence support. It reinforces the complexities of the LIC environment, constantly fluctuating from macro-to micro-analysis.

The paper features a lengthy illustration of the use of intelligence systems and communications to provide intelligence support to a LIC scenario in several different models. The Battle Command Training Program (BCTP) has a viable application to the LIC environment. The conclusion offers a logical approach to operationalize the concepts set forth in the paper.

Five Imperatives

> "In a new era there are also new tasks and new priorities. Regional turmoil will place growing burdens on intelligence collection, processing and analysis. At the same time, we must track the threats posed by narcotics trafficking, terrorism and the proliferation of advanced weapons. We must also be more fully aware of international financial, trade and technology trends that could affect the security of the United States, including its economic well-being."[11]

In order to insure that all policy and operational concerns in LIC are adequately covered by intelligence resources, proponents of LIC must understand that intelligence requirements for national systems are competing with all other national requirements in order of priority, This can be accomplished in a painless manner, provided strict adherence to the following LIC intelligence support imperatives.

The first of these imperatives, the overriding requirement for any LIC scenario, is *cognitive intelligence* to insure force protection of all U.S. forces. This country can not stomach another incident like the Marines experienced in Lebanon.

The second imperative mandates that the intelligence support be *adaptive* in nature. This simply means that the intelligence must be easily adopted by the host-nation into its intelligence process. It must be readily usable by host-nation decision-makers and commanders.

Much of the information to be used in a country assessment is unclassified data. The availability of unclassified data will likely continue and expand in the future. Thus, the third imperative is to *use open source material* as the foundation for the economic, political, social, and geographical data bases.

The fourth imperative requires the intelligence preparation of the battlefield (IPB) products be *tailored to mission* activity. This will prevent the system from generating all IPB products for every mission activity. The consumer will gain a better appreciation for

intelligence support if mission-specific products are issued, rather than every analytical product on the area requiring a time-consuming and confusing filtering process.

Assured communications—the fifth imperative— is a requirement that will guarantee worldwide connectivity, as opposed to localized or theater connectivity only. Dedicated communications is not needed. The same connectivity can support conventional warfare and LIC operations. Intelligence depends upon communications, but connectivity should not require major reconfigurations every time forces deploy. Communications will be discussed at length in the latter part of this paper.

By routinely following five imperatives, the intelligence community can be used more productively to work critical issues and provide meaningful and useful answers, because the right query was made and disseminated properly. While there is nothing new about these imperatives, perhaps they have not been thought of as linked in this fashion and specifically oriented to the LIC environment. Intelligence requirements for any given LIC situation may compete with more pressing requirements. The five imperatives should preclude routine requirements for being elevated to the national level.

Ten Principles of Intelligence Support to LIC

Intelligence support to the LIC environment should always adhere to the following principles. These principles have taken into consideration that the intelligence support frequently may be provided by deployed resources. The long term intent is to build an intelligence capability to fulfill the country's intelligence requirements to counter or exploit any threat, as well as to identify potential threats.

The first principle is *initiative*. Intelligence must always provide before-the-fact information. The intelligence process must be proactive, rather than reactive, in nature. The process must demonstrate both a predictive and a cognitive nature.

Adaptability, the second principle, takes existing intelligence procedures and looks for parallels, or corollaries, to discover a method to best portray the current situation by modifying existing procedures.

The third principle is *flexibility*. The quality of the intelligence support must not vary whether it is remoted from the continental United States to a host nation or it is being collected and produced in the host country. The data bases should be common and easy to manipulate.

The most important principle is *exportability*. The intelligence collection systems, communications, and automation (hardware and software) must be usable, easily operated and maintainable by the host nation. Otherwise, the U.S. will merely burden the host nation with a capability that will be useless as soon as the U.S. withdraws from the LIC engagement.

The intelligence support should be designed in such a way that each echelon of intelligence, to include within the host nation system, is *complementary* rather than redundant, in nature. This technique allows more targets to be covered rather than more coverage on a specific target. Within a given echelon, multiple collection assets may be

appropriate. This technique does not detract from the theory of collection assets "cueing."

Intelligence support must be able to guarantee *specificity*—the sixth principle. Counterterrorism, evacuations of non-combatants, hostage rescue, and some other special operations missions require very specific intelligence. This kind of information must constantly be improved and updated. The principle of initiative must augment specificity to indicate where these type special operations actions may happen—predictive intelligence.

That which binds all the principles together is the seventh principle—*validity*. Intelligence support must remain valid through execution of the plan, or option. What was accurate and timely yesterday may not be valid at H-Hour (e.g., Son Tay Raid). The intelligence planners and analysts must be able to update the intelligence picture through mission completion. Intelligence is not a "fire and forget" weapon system.

Reliability, the eighth principle of intelligence support. Both the intelligence product and the means to disseminate the product must be reliable to keep the confidence levels high. The support system can not afford to lose a link without a backup means at a critical time.

The ninth principle is *tech-capable*. The intelligence system must be able to sample the environment and decide what tech-capable (low, medium, high) collection systems are required to exploit the environment. The intelligence and electronic warfare systems provided the host nation through security assistance should be plug-in/plug-out type systems to allow the platforms to serve multi-purposes. The host nation must be allowed to get as technologically sophisticated as the threat.

The tenth and final principle of intelligence support to LIC is user-friendly *verification*. This applies to everything from mobile training teams, collection systems, automation (hardware and software), power systems, and liaison elements. The host nation must

completely understand and demonstrate proficiency of all the systems and procedures in order for their usefulness to be appreciated.

Perhaps these principles are slanted for the convenience of the host nation. But as a reminder, the host nation is our customer and it has always been good business ethic to leave your customer happy.

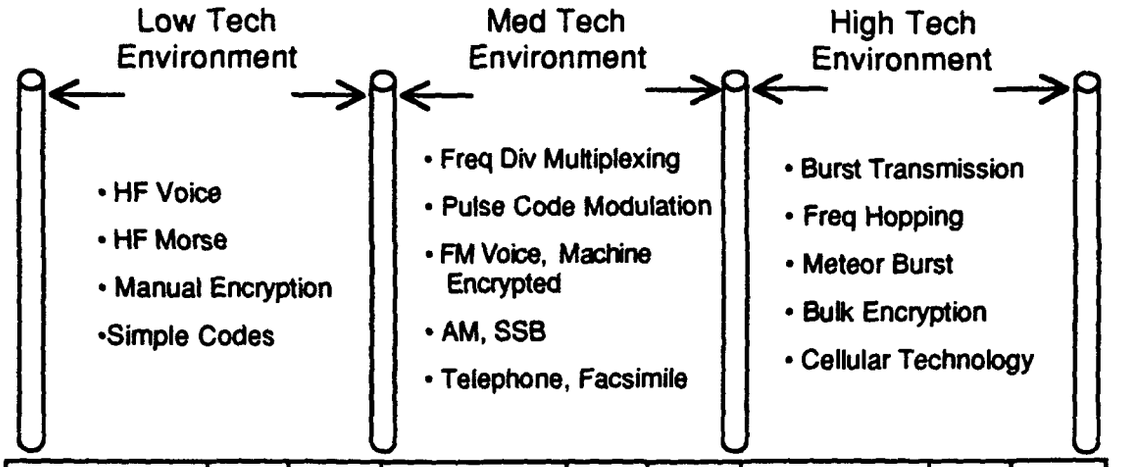
Intelligence Capability Spectrum

In addressing how best to use intelligence to assist in achieving U.S. national policy in the LIC environment, an intelligence capability spectrum must be continuously refined and used as the start point in policy formulation (Figures 1, 2, and 3). The intelligence capability spectrum of each host nation must be evaluated to determine the sufficiency of collection systems to cope with the area threat. If upgrading of a host-nation's intelligence system is required, the sophistication of the system must be of such a nature that it is commensurate with the skills of the host-nation operators.

Too often, the Army's senior leadership takes a rich man's approach to war, viewing access to technology as offering a significant comparative advantage over potential adversaries.[12] The old mindset of the rapid deployment of massive U.S. military forces to a hostile area employing state-of-the-art technology to defeat an enemy force will be the exception, rather than the rule. The chances of U.S. military maneuver forces being committed in a LIC situation are small.[13] The U.S. role more likely will be one of support and assistance, rather than direct intervention. Military responses and options are limited. Aggressive force would, in many scenarios, prove ineffective, unacceptable, or counterproductive as a response.

In the LIC environment, host-nation intelligence support must be technologically sophisticated enough to satisfy the decision-makers' intelligence capabilities to exploit both ends of the spectrum of LIC environments and flexible and adaptive enough to operate in the least sophisticated host-nation intelligence process until a better capability can be developed.

SIGINT



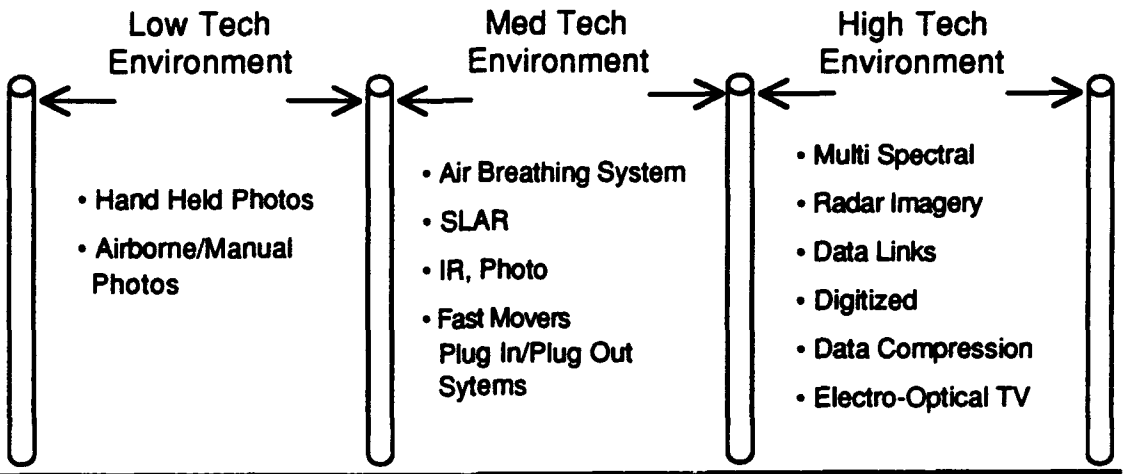
Areas of Concern	Assessment:	T	S	Assessment:	T	S	Assessment:	T	S
Econ	NT	NA	NA	PT	NA	CD	PT	NA	CD
Pol	NT	NA	NA	PT	CD	CD	PT	CD	CD
Soc	NT	NA	NA	NT	NA	NA	NT	NA	NA
Psy	NT	NA	NA	NT	NA	NA	NT	NA	NA
Geo	NT	NA	NA	NT	NA	NA	NT	NA	NA
Mil	TGT	CC	CR(-)	TGT	CC	CR(-)	TGT	LC	CR(-)

Legend:

- T = Tactical Collection
- S = Strategic Collection
- NT = Not Targetable
- NA = Not Applicable
- TGT = Targetable
- CC = Continuous Coverage
- CR(-) = Coverage is Possible Revisit Time is Questionable
- PT = Possible Target
- CD = Coverage is Possible but Difficult
- LC = Limited Capability
- PC = Partial Coverage

Figure 1. Intelligence Capability Spectrum Matrix

IMINT



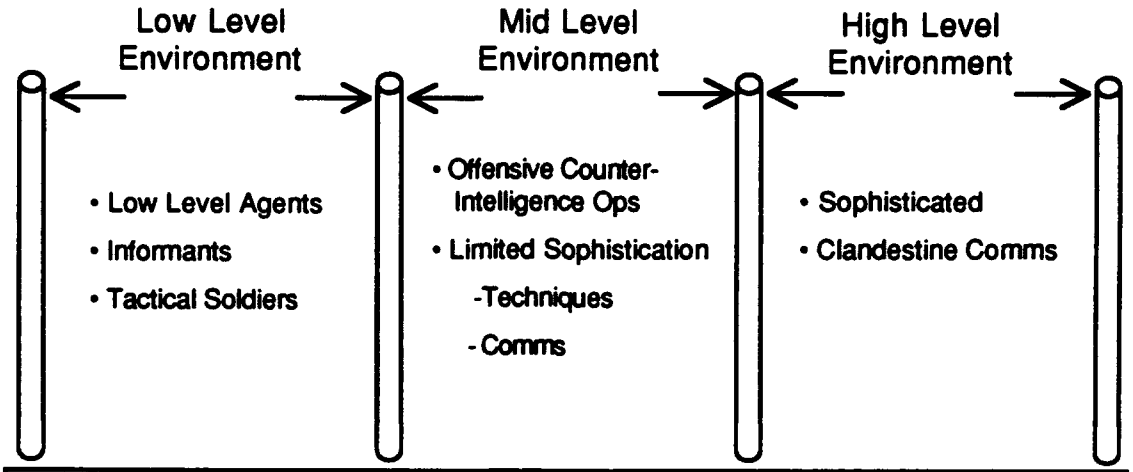
Areas of Concern	Assessment:	T	S	Assessment:	T	S	Assessment:	T	S
Econ	NT	NA	NA	NT	NA	NA	NT	NA	NA
Pol	NT	NA	NA	NT	NA	NA	NT	NA	NA
Soc	NT	NA	NA	NT	NA	NA	NT	NA	NA
Psy	NT	NA	NA	NT	NA	NA	NT	NA	NA
Geo	PT	LC	NA	TGT	PC	PC	TGT	NA	CR(-)
Mil	PT	CC	NA	TGT	CC	PC	TGT	NA	CR(-)

Legend:

- T = Tactical Collection
- S = Strategic Collection
- NT = Not Targetable
- NA = Not Applicable
- TGT = Targetable
- CC = Continuous Coverage
- CR(-) = Coverage is Possible Revisit Time is Questionable
- PT = Possible Target
- CD = Coverage is Possible but Difficult
- LC = Limited Capability
- PC = Partial Coverage

Figure 2. Intelligence Capability Spectrum Matrix

HUMINT



Areas of Concern	Assessment:	T	S	Assessment:	T	S	Assessment:	T	S
Econ	PT	PC	PC	TGT	PC	PC	TGT	NA	CC
Pol	PT	PC	PC	TGT	PC	PC	TGT	NA	CC
Soc	PT	PC	PC	TGT	PC	PC	TGT	NA	CC
Psy	PT	PC	PC	TGT	PC	PC	TGT	NA	CC
Geo	TGT	PC	PC	TGT	PC	PC	TGT	NA	PC
Mil	TGT	CC	PC	TGT	CC	PC	TGT	NA	CC

Legend:

T	=	Tactical Collection
S	=	Strategic Collection
NT	=	Not Targetable
NA	=	Not Applicable
TGT	=	Targetable
CC	=	Continuous Coverage
CR(-)	=	Coverage is Possible Revisit Time is Questionable
PT	=	Possible Target
CD	=	Coverage is Possible but Difficult
LC	=	Limited Capability
PC	=	Partial Coverage

Figure 3. Intelligence Capability Spectrum Matrix

Shedding the Conventional Mindset

> "To simply study the battlefield and the deployment of enemy forces in conventional military terms is to leave undone the bulk of the intelligence analysis required for low intensity conflict environments. This is because of the unique, varied and complex requirements for analysis in LIC, as opposed to the more concrete and straightforward requirements of conventional warfare."[14]

Two problems confront the U.S. Army in dealing with intelligence support to LIC operations. First is the ability to transfer intelligence procedures and requirements from the conventional battlefield to the LIC environment. The second problem is the identification of the information required. These problems arise because Army planning for conventional battlefields has accustomed commanders, staff officers, and intelligence analysts to the type of information needed to cope with the Soviet threat and to anticipate battlefield intelligence requirements associated with Soviet tactics, techniques, procedures, and doctrine. Such institutional training and experience does not exist to the same extent for LIC.[15]

The simple pretext that training is a technique that can be easily conveyed and mastered provided a solid foundation in basic principles are present and understood does not hold true in the intelligence business.[16] The complexities of intelligence requirements in LIC operations make the old conventional Soviet scenario look like a "set piece."

In the future the U.S. Army can expect a LIC environment which bears no resemblance to its conventional counterpart. Success in the conventional arena has always been measured in terms of deterrence and defeating the enemy forces in battle. In the LIC environment success is measured in terms of achieving U.S. national objectives without protracted combat commitment of U.S. forces. LIC targets will be more difficult to identify than the second echelon of a Soviet tank division. Doctrinal

templates will be useless in most LIC situations. Intelligence preparation of the battlefield (IPB) must address a broader range of political, economic, social, geographical, and military factors in LIC.

Even though there is currently a doctrinal void in the intelligence community to adequately address intelligence support to every possibility along the operations continuum, there is a school of thought which insists that the void can easily be overcome by adapting and modifying conventional techniques to LIC requirements.

> "LIC to include counternarcotics operations, does not require abandonment of our doctrine. This is especially true in intelligence. What does change is how we apply our intelligence and electronic warfare doctrine in the LIC environment. Our intelligence products will differ based on the commander's requirements in different LIC scenarios and our terms of reference may vary. However, the criticality of intelligence throughout all components of LIC cannot be overemphasized. Indeed, if intelligence and security assistance are correctly applied in the earliest possible stages of LIC the large scale commitment of U.S. forces can be avoided."[17]

This demands a "mindset transfer," which requires more initiative and professional depth than was previously required in the conventional setting. There is neither the time nor the resources to replicate a different set of techniques and procedures to address LIC scenarios. In making the transfer to the LIC mindset, the following factors must be completely understood:

1) The *limitations of high-technology* in some LIC scenarios.

2) In most cases, the LIC environment demands a heavy *dependence of human intelligence (HUMINT).*

3) In most cases, the *objective is not destruction* of the enemy forces.

4) *Intelligence focus can not be limited* to military capabilities and intentions. The scope must include intelligence preparation of the area to cover political, economic, social, and geographical factors.

5) The nature of LIC dictates an *emphasis on intelligence planning, coordination, collection, and dissemination.* The integration of U.S. and host nation production should be routine.

6) The *threat is intrinsically civil-military*, regardless of how ambiguous and complex.[18]

This intelligence preparation of the battlefield, operational area, or target area must be broad enough in scope to cover all the inherent LIC factors, yet be capable of being tailored to aid in formulation of plans for specific mission activities in LIC operations. Intelligence preparation must be conducted with a LIC mindset in order to maximize military intelligence as a vital instrument in the formulation of successful U.S. policy. Examples of the "mindset transfer" are illustrated in Figures 4, 5, and 6.

Terminology	Context	
	Conventional	LIC
Operational Level	Army/Corps	Company/Platoon
Key Terrain	High Ground	Population Centers
High Value Target	1) 2d Echelon 2) Assembly Areas	1) Drug Processing Lab (Counternarcotics TGT) 2) Sugar Factory (Econ)
Doctrine	Written Doctrine	NA
Doctrinal Templating	1) Existent 2) "Cookie Cutter" Approach	1) Non-Existent 2) Pattern Analysis 3) Reactive Doctrinal Template ("Adaptive" Templating)
Lines of Communications	Easily Detectable	Not Easily Detectable
Orientation	Military	1) Economic 2) Political 3) Social 4) Geographical 5) Military
Use of Military Force	Expected; Required	Not Always the Best Solution
Situation Development	Disposition of Enemy Forces; Military Capabilities and Intentions	Patterns of Operations, Current and Projected; Political Activity; Social Development; Popular Support

Figure 4. Mindset Transfer Matrix

The IEW Synchronization Matrix in LIC

The purpose of the IEW synchronization matrix[19] is to focus all collection, production and dissemination effort on the commander's intelligence requirements. The IEW synchronization matrix is applied after the operations plan is well developed and an execution matrix is available. (Top portion of Figure 5 shows the execution matrix.[20]) This matrix contains operational events, decision points, and timelines. Together these identify key times in the battle when critical friendly events will occur. The intelligence staff must understand the matrix completely to successfully anticipate the commander's requirements.

The next section of the matrix consists of time-sequenced preplanned priority intelligence requirements. Preplanned priority intelligence requirements are what we expect the commander's future priority intelligence requirements (PIR) to be as the operation develops.[21] (Bottom portion Figure 5 shows preplanned PIRs.)

After establishing the preplanned PIRs along the bottom of the matrix, we can backward plan collection, production, and dissemination efforts to answer the PIRs.[22] On the synchronization matrix, this is represented by an intelligence collection schedule. The collection schedule is in the center of the matrix. The collection schedule shows the planned coverage times of the various collectors. The collection times are influenced by the requirement to answer the commander's PIRs and not by the agency or unit owning the assets.

Application of the IEW synchronization matrix is also feasible in a LIC environment. Whereas in the conventional setting it interacts between the friendly operational events and the commander's preplanned PIR, in LIC it interacts between future possibility of enemy activity reported by intelligence sources and pattern analysis to determine operational options to deny, exploit or destroy the enemy.

For instance, a low-level agent reported that insurgents plan to sabotage a refinery at 2200hrs on Day 4. (See Figure 6.) By looking in the incidents data base under "sabotage," the following pattern analysis appears for over 15 sabotage incidents. The next step is to plot on the matrix incidents that occurred over the last 72 hours even though the pattern only reflected a reference 24 hours from execution. Review all incidents to see if there is any possible linkage. In this case focus on the incident and the engineer platoon. Try to discern if the incidents fit the pattern or were staged to conceal the real target. Ask questions: How many shots were fired? Did they obtain or ask for demolitions? If so, what quantity did they obtain? Intelligence has to take the investigative approach similar to homicide detectives.

Now, the focus is on the pattern to see how many pattern events have not occurred. After this analysis, the effort is directed on events that can still be influenced. In this situation there is still time for counter-reconnaissance and counter-surveillance patrols, mounted patrols checking IPB ambush sites, and finally deny access to all refineries, a very expensive option.

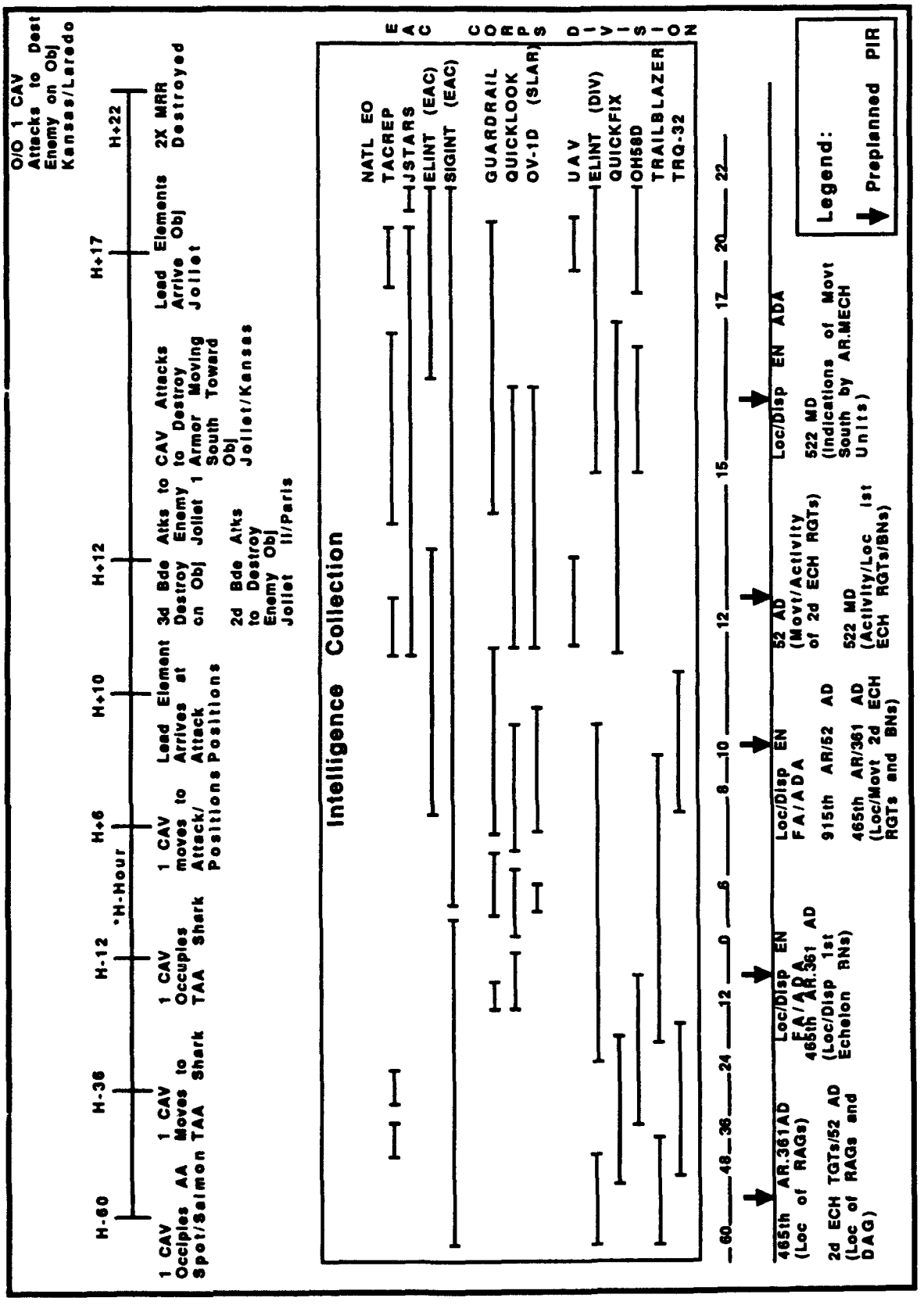


Figure 5. The 1st Cavalry Division IEW Synchronization Matrix ("Razor's Edge")

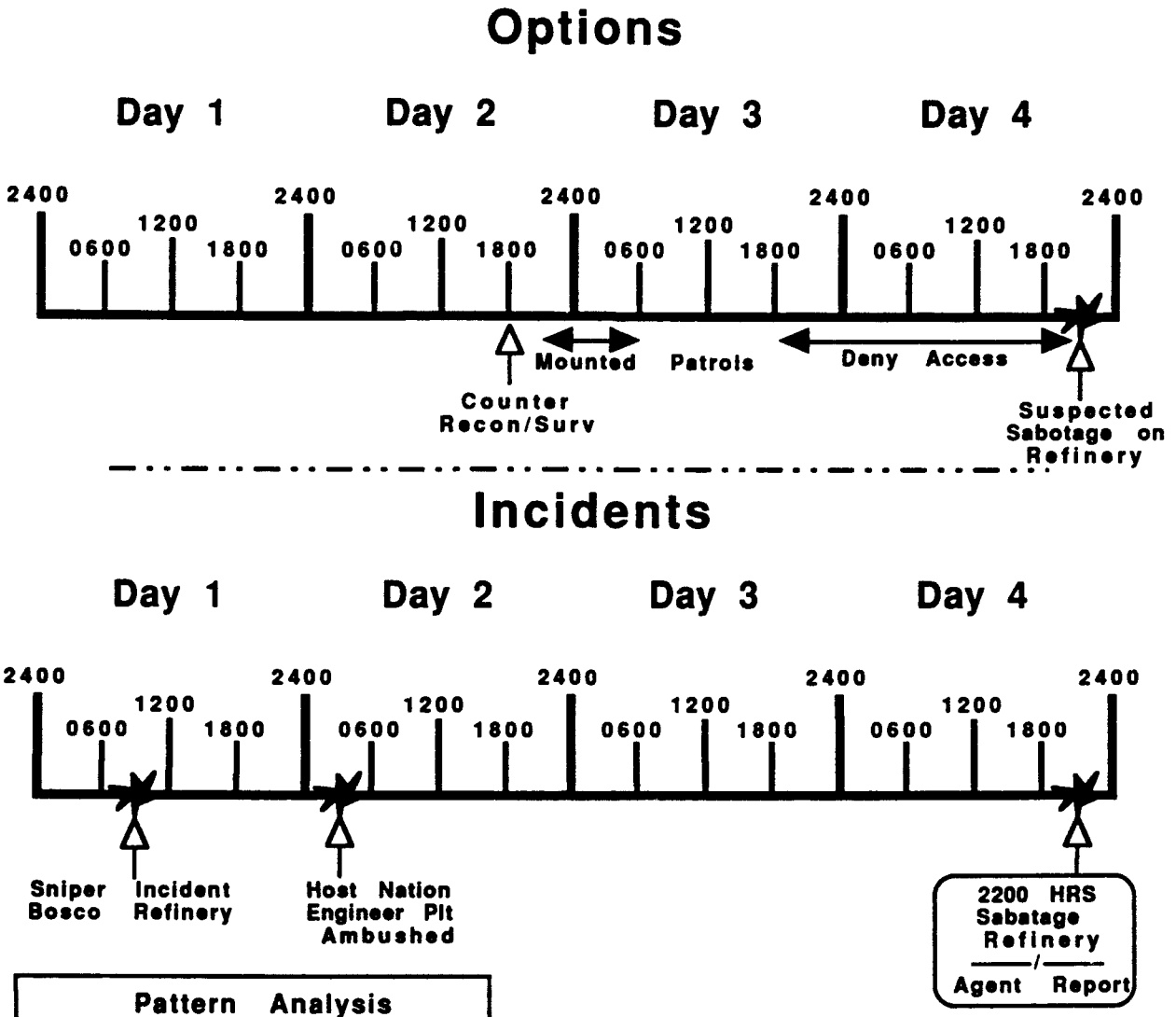


Figure 6. IEW Synchronization Matrix in LIC

Intelligence Data Bases

The approach of establishing data bases on social, political, military and geographic factors is an excellent start point to the analytical process of identifying trends, vulnerabilities and commonalties in regions of a country. Much of this data can be obtained through open sources and debriefings of U.S. citizens , especially from the private sector traveling abroad for personal and business reasons. It should be noted, however, that without some sort of filtering process even this becomes extremely resource intensive. The data bases at a minimum should be able to provide meaningful data[23] on the following issues:

Economic Data Base

1) Economic target most vulnerable to attack.

2) Economic conditions most vulnerable to psychological exploitation.

Social Data Base

1) Vulnerability of population to exploitation.

2) Identity of true motives of discontent in order to treat the causes not the symptoms.

Political Data Base

1) Viability of the current regime.

2) Extent to which U.S. forces will be allowed to operate (i.e., will the presence of U.S. forces be limited to civic actions?).

3) Identity of contending political parties and factions.

4) Verification of the host nation's true objectives.

Geographical Data Base

1) Routine terrain studies.

2) Use of urban terrain by the threat.

3) Use of rural areas for cover and concealment by the threat.

4) Location of all cultural geography (dams, power lines, power stations, railroads, bridges, factories, etc.).

Military Data Base

1) True relationship among the host nation military, police, and civilian government.

2) Military capability to counter the threat.

3) Capability to operate and maintain intelligence and electronic warfare security assistance materiel.

4) Vulnerabilities to psychological operations.

It is important to understand that the LIC threat cannot be adequately assessed in the conventional terms of composition and disposition of combat forces, key terrain, avenues of approach, time distance factors, and doctrinal/situational templating. Instead, LIC intelligence requirements[24] must focus on:

1) Non-conventional situational cues (political, social, economic, and psychological).

2) The root causes of the conflict.

3) The degree of popular support for the threat and for the host nation.

4) Threat strategy, intentions, capabilities and vulnerabilities.

5) Host nation counter-threat capabilities.

6) The identification of potential courses of U.S. action.

Again, U.S. forces will probably not be employed in a dominant or independent role but in a multi-faceted supporting role. This makes it necessary for military intelligence analyses to be as current and thorough as possible in terms of economic, social, political, geographical, and military factors. No one of these factors is more dominant than the other.

Intelligence: The Common Thread in All LIC Operations

Some form of intelligence is an essential component of every LIC scenario. The specificity of intelligence requirements range from micro to macro depending on the type of LIC operation. The intelligence support to the complete array of LIC operations is by far the most challenging requirement facing the intelligence community in the future. In this environment, technology is often unable to provide the huge collection payoffs as in conventional warfare. Therefore, intelligence procedures for both collection and analysis must be adaptive in nature. This is particularly necessary when noting that the operational level in these type engagements, specifically insurgency and terrorism, may be at the platoon or company level.[25]

JCS Pub 3-07, outlines intelligence support to LIC as follows:

Insurgency. Accurate, timely intelligence is essential. United States national and theater intelligence agencies are a source of intelligence otherwise unobtainable by the resistance movement. In return, the resistance movement may be able to provide the U.S. Armed Forces with technical and order of battle intelligence. Such intelligence support will include a feedback and effectiveness reporting mechanism.

Counterinsurgency. Intelligence provides the basis for all U.S. and host nation counterinsurgency plans and operations. Potential intelligence consumers involved in counterinsurgency planning include host nation forces, the U.S. country team,[26] the U.S. combatant commands, a joint task force, military assistance advisory group, and security assistance organization commander/director, and the National Command Authorities. Where elements are those of the host nation, collection capability depends solely on human intelligence (HUMINT). Additional intelligence may help, but diplomatic and internal political considerations will often limit U.S. Armed Forces intelligence operations until the need for a larger U.S. Armed Forces role is determined. As a result, integration of non-military United States HUMINT effort, exploitation of U.S. technical

collection resources, and sharing of resultant information as appropriate will collectively constitute principal elements in intelligence support.

Terrorism. The intelligence and counterintelligence components of the Military Departments, the Defense Intelligence Agency (DIA), and the National Security Agency (NSA), or designees, ensure prompt dissemination of intelligence information on terrorist threats. This information is disseminated routinely by the Military Services, DIA, and NSA to DoD components which have personnel traveling to foreign countries by apprising them of the general terrorist threats they may encounter. The DoD also has specialized forces to deal with the terrorist threat.

Intelligence is the first line of defense in combating terrorism. A well-planned, systematic, all-source intelligence program is essential to identify the threat and provide timely threat warning. This includes evaluation of terrorist capabilities, tactics, and targeting strategy, and the dissemination and sharing of this information with all interested and affected agencies and organizations. Coordinated management of intelligence requirements will facilitate counterterrorism operations and will serve to preclude intelligence gaps.

Peacetime Contingencies. Intelligence is a particularly critical part of these types of operations. The rapid introduction of U.S. combat forces requires planning. The rapid introduction of U.S. combat forces requires planning. Accurate, detailed, tailored, and timely all-source intelligence can determine the success or failure of these operations. Time for planning and execution is typically short, and intelligence assets must anticipate requirements and provide comprehensive products on extremely short notice. The ever increasing demand for intelligence to support low intensity conflict and all other worldwide requirements makes the management and control of intelligence resources crucial. Timely, accurate information is essential to the decision making process.

Even in peacekeeping operations, certain tasks will be levied upon the intelligence community concerning, *interalia*, demographics of the area (a macro area analysis) and

terrorist activity. U.S. force protection will stimulate the bulk of the intelligence requirements. Peacekeeping forces should be briefed on outstanding intelligence requirements easily obtainable by soldiers performing this type of mission. Detailed debriefings should be conducted upon the return of the peacekeeping forces to determine if any of the data base factors can be updated.

Due to the broad spectrum of LIC possibilities, logistic intelligence is critical to the LIC planning effort.[27] The provision of the necessary intelligence will be facilitated by long-range preliminary planning to include area studies and target information folders. Such logistic intelligence should include, as a minimum, the following:

1) Intent to engage in combined operations and/or extent of logistical support to non-Department of Defense agencies and /or allied forces.[28]

2) Available resources in the area of operations as well as facilities to stockpile materiel.

3) Conditions which alter the consumption factors, e.g., jungle, desert, or Arctic conditions.

4) Foreign military logistic structure and national infrastructure capabilities.[29]

5) Information on the capability of local facilities to support reception and sustainment operations.

6) Environmental, geographical, climatological, and topographical factors that may affect logistical operations.[30]

7) Analysis of the capabilities of the host-nation's and region's lines of communication and the U.S. strategic lines of communication and capabilities to support the LIC operation.

8) Dimensions of other external support to the supported country or movement's forces and to adversary forces.[31]

9) Information on weapon systems and equipment interchangeability and interoperability.[32]

Accurate, timely, and reliable intelligence is the most important factor when responding to low intensity conflict. This applies to framing a response and executing a plan. Intelligence assists in the forming of an assessment of a particular country's political, military, economic, and social conditions. The assessment becomes the basis for the *decision to aid* a country and exactly where and in what quantity to apply that aid. Intelligence must monitor and the aid program's progress and the actions of the opposition. Finally, intelligence estimates will support the *decision to terminate* the program.[33]

Intelligence is key to the successful formulation and implementation of any viable U.S. policy in the LIC environment. The proper positioning of the limited intelligence assets and resources is a significant challenge that must be overcome if military intelligence will function as a military instrument, a vital element, and a common threat that bind together viable U.S. options in all LIC scenarios.

Battle Command Training Program (BCTP) for LIC

With necessity being the engine of change, it is both fitting and proper to expand the BCTP concept to include the LIC environment. The payoff from this approach will be extremely high for both the country team and the military.

The immediate payoff of expanding BCTP to exercise the players in LIC operations will be the "mindset transfer" from conventional operations to LIC operations. The adaptive process required in order to achieve success in LIC operations in this setting will take place in the game area and not in the insurgent's or terrorist's area.

This "mindset transfer" must occur within all the players: country team, national agencies, and the military. This transfer will definitely facilitate the understanding of the intelligence product. The user/consumer must understand the product. A trust in the intelligence product by the user must be developed early on. The user, as a player, must learn how to stress the intelligence system to gain the best intelligence possible in order to develop the best possible policy options. To aid this process the intelligence capability spectrum and the mindset matrix must be user-friendly and easily understood by military and non-military personnel. Again, by simply adjusting the mindset in a LIC versus conventional environment, the BCTP concept can be applied to exercise the entire gamut of LIC components, specifically the intelligence procedures and products unique to each of the LIC components.

The feasibility of using A BCTP-type program to identify system shortfalls, staff/agency weaknesses, intelligence gaps, data base inadequacy, and as a systematic approach to stimulate the mindset transfer makes this approach more than appealing. By exercising the military and national agencies, a better assessment of the current policy can be realized. Priorities for the future could be established, and perhaps this type of forum would make it easier to obtain a consensus in developing future courses of action.

If military intelligence is a vital element that supports U.S. interests, logical steps must be taken to seek ways to get involved early by helping appropriate nations build a military intelligence capability before they are faced with a crisis.[34] We must focus on early detection of crises and seek peaceful solutions.[35] Before commitment of U.S. assets, it is imperative that all doctrinal deficiencies, interoperability issues, automation shortfalls, capability gaps, LIC priorities by region, and mindset transfers are identified and rectified as rapidly as possible. A BCTP-type program for LIC would definitely level the playing field for a new beginning with some mindset adjustments.

A Different Approach

In order to maximize the efforts of our shrinking intelligence assets, especially at the corps level and below, a brief pause should be taken to evaluate what is happening, what is not happening and how to best influence the action.

First, let's consider what is happening. There are analysts at corps and division level without a focus since the fall of the Soviet Union. It is obvious what is *not* happening. No one has figured out how to gainfully employ these valuable assets. Rather than gear analytically to fight "Blueland" and Greenland," why not focus on a LIC potential flash point.

The difficulty is how best to influence the action. This can best be done by allowing the regional Unified Commander-in-Chief (CINC) access in the form of intelligence tasking authority for all forces assigned to him for contingency operations. By requiring the intelligence units to work intelligence-related issues as prioritized by the J2 in coordination with the country teams, the intelligence data bases could be significantly enhanced. This would increase the success in the predictive intelligence arena.

Realizing the world is a large place, there has to be a way to narrow our focus. Through national/regional assessments potential flash points could be identified. The intelligence effort can focus on these potential flash points. If the consensus is that the flash point is adequately covered with current collection assets as well as data base files and maps, the J2 can assign lower priorities. Getting the CINC involved is key. The obvious positive result of this approach is that the CINC will eventually have better intelligence for his entire region.

In order for this approach to work there must be very little redundancy and increased complementary intelligence production between echelons. The force structure to allow this to happen is already in motion. There will be dedicated Army intelligence production elements in each Joint Intelligence Center or JIC.[36] The Corps Military Intelligence

Support Elements (CMISE) are also being formed. The CMISE mission is to reinforce each corps' collection and production capabilities. CMISE assumes the complementary production mission. The CMISE is a concept which combines soldiers funded by strategic/echelons above corps funds (Major Force Program 3) with soldiers assigned to corps and divisions (Major Force Program 2).[37] This is a multi-discipline organization (SIGINT, HUMINT, IMINT, and CI) which will develop intelligence in direct support of corps commanders' priority intelligence requirements, which should be tied to the flash points that the CINC assigned the corps to work. This organization is assigned to U.S. Army Intelligence and Security Command (INSCOM) and will provide direct connectivity to ongoing real-world collection operations conducted by theater military intelligence brigades in regions of interest to the corps. This organization will also give corps access to other CONUS-based and national-level intelligence operations.

> "As budgets are reduced, we believe the DoD/National Community will provide less tactically-oriented intelligence for peacetime planning. Thus, we must face reality and maximize the potential for out tactical soldiers to help fill this void. To this end we developed the concept of the Corps MI Support Element or CMISE."[38]

At an installation like Fort Lewis, Washington, this means that there is a Military Intelligence Brigade, Military Battalion (CEWI), Corps G2 staff, Division G2 staff, and CMISE. This equates to over 260 analysts in addition to collectors. This organization is robust and has the required structure to handle all the requirements the J2 can levy on flash points as well as long as they are recipients of the intelligence from the required sources.

A Feasible IEW Architecture

During Operation Just Cause, Desert Storm/Desert Shield, and Operation Provide Comfort, the U.S. proved that through system remoting, near-real time data links, and reliable high speed communications that there is no longer a requirement to have the intelligence analysts collocated with the operational decision makers. In LIC engagements, this method is rapidly becoming the rule rather than the exception. This will remain the preferred method of intelligence support, because the intent is to provide quality intelligence to the host-nation in order to develop viable courses of action to deter or defeat any security challenges to its economic or political well-being.

This IEW architecture has captured the essence of the five imperatives, the ten principles, and the intelligence capability spectrum matrix. The model also shows the capability to support both conventional warfare and LIC engagements without requiring major modifications. This architecture can be exercised frequently by real-world intelligence requirements, exercises, and during humanitarian assistance operations in the region. The primary focus of this architecture is from the Unified Command to the most forward-deployed element (host-nation or U.S. forces).

The obvious advantage of this IEW architecture is that the formats, routers, system protocol, cryptography devices, and alternate routing procedures will not change during a crisis situation. This alleviates the risk involved in establishing a complex communications architecture during a crisis situation. The time involved in bringing the communications system on-line, coupled with operator train-up time, can cause a long delay in processing valid and perishable intelligence requirements.

All intelligence players become extremely comfortable with the IEW architecture while manipulating data bases, answering queries, cueing collection systems, reporting new threat capabilities, and updating taskings in a "stress free" environment. Familiarity prior to a crisis significantly enhances the probability of success during the crisis.

Assured communications will always increase the confidence level of the intelligence community.

The required operational capability for this IEW architecture had to satisfy three capability parameters:

1) Accommodate *SIGINT, HUMINT, and IMINT requirements.*

2) Take advantage of intelligence systems with on-board embedded communications.

3) *Maximize space technology* for taskings reporting, and dissemination as well as collection.

> "We must provide deployed commanders, through existing command and control mechanisms when possible, real time, accurate, fused intelligence tailored to the local threat."[39]

This IEW architecture conforms to the mandate in the above quotation from LTG Williams when he was the Director, Defense Intelligence Agency in 1984. Figure 7 illustrates the relationships among key components and with their intelligence support.[40] Figure 8 graphically shows the echelons with the IEW and communications means to drive intelligence. Figure 9 displays the means available for processing and disseminating ELINT. Figures 10, 11, and 12 display the means available and connectivity for processing and disseminating COMINT, IMINT, and HUMINT, respectively.

This architecture will support both in-country and out-of-theater intelligence support requirements. This same architecture can support a Joint Task Force (JTF) even in a split-operations intelligence mode if required (half in CONUS and half in-country). Every system shown in the IEW architecture is currently fielded. To make this system work will require some collocation or communication system-sharing between elements depicted at same location but not organic to the same unit. This potential obstacle can be

eliminated by a J2 with intelligence tasking authority of intelligence assets assigned to his CINC during a regional conflict.

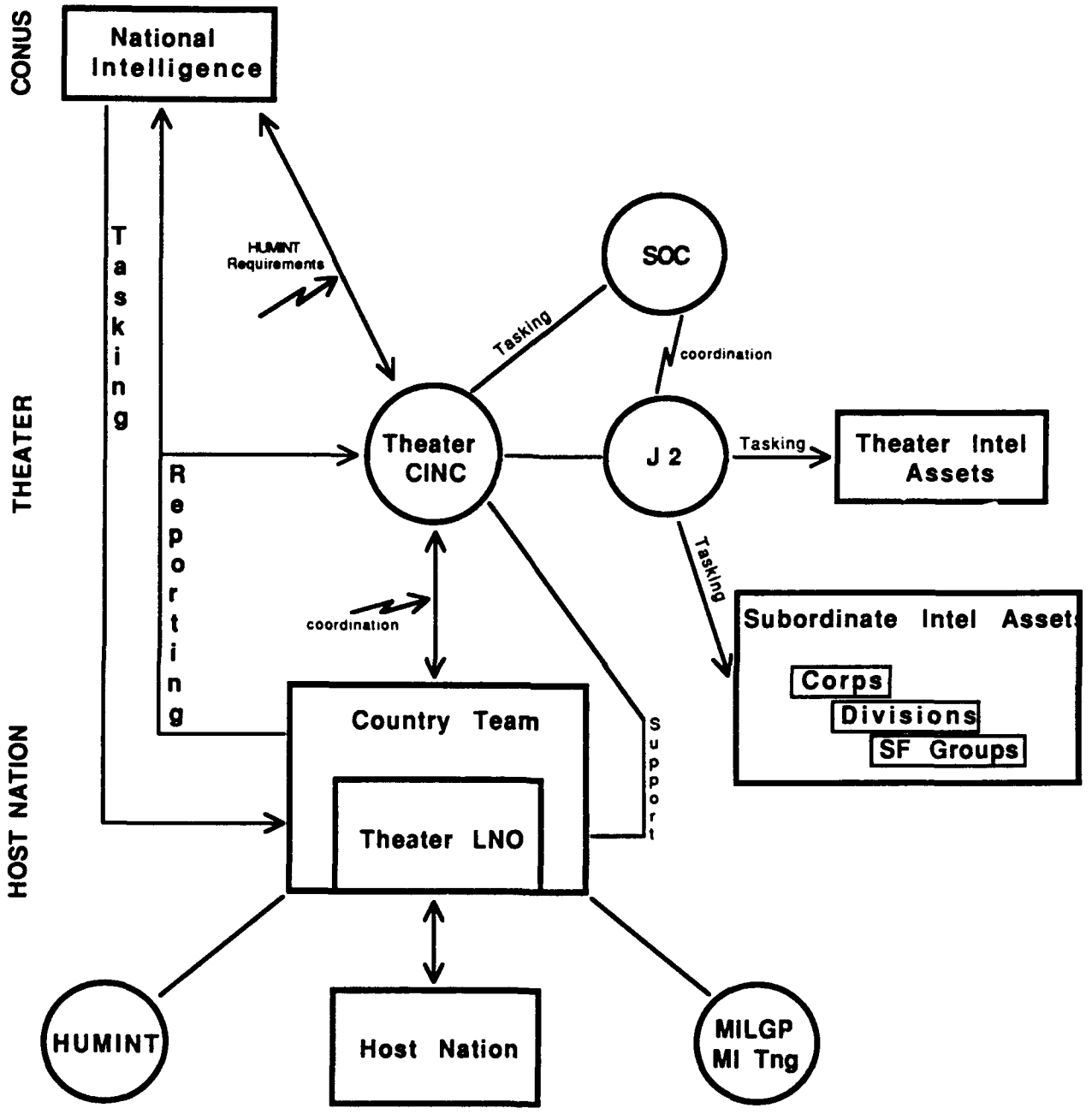


Figure 7. IEW Architecture

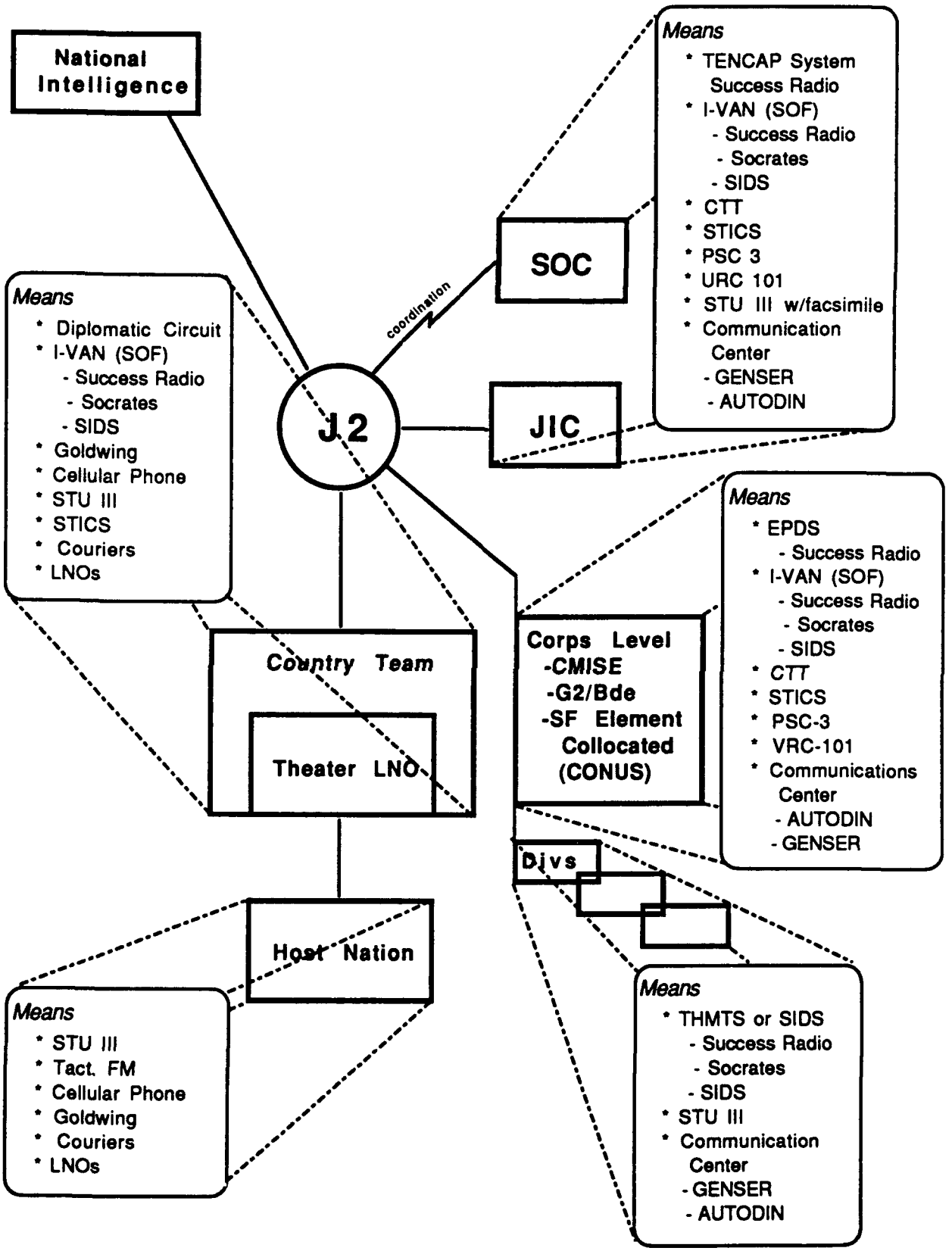


Figure 8. IEW Architecture

ELINT

	Success Radio*	AUTODIN	PSC 3	URC 101	STU III	Goldwing	Courier
National Level	X	X			X		
Theater J2	X	X	X	X	X		X
Corps Level	X	X	X	X	X		
Country Team	X		X		X	X	X
Host Nation					X	X	X

* Note: Success Radio capabilities to communicate with
- Quicklook
- Rivet Joint
- Tadixs B Broadcast
- Flt/AF SATCOM
- Point-to-Point Terrestrial

Figure 9. IEW Architecture

COMINT

	Success Radio	AUTODIN	SOCRATES	PSC 3	URC 101	CTT	STU III	STICS	Goldwing	Courier
National Level	X	X	X				X	X		
Theater J2	X	X	X	X	X	X	X	X		X
Corps Level	X	X	X	X	X	X	X	X		
Country Team	X		X	X			X		X	X
Host Nation							X		X	X

Figure 10. IEW Architecture

Digitized Imagery

	Success Radio	SOCRATES	AUTODIN	Commercial Phone	Courier
National Level	X		X	X	
Theater J2	X	X	X	X	X
Corps Level	X	X	X	X	
Country Team	X	X			X
Host Nation					X

Figure 11. IEW Architecture

HUMINT

	Success Radio	AUTODIN	SOCRATES	PSC-3	URC 101	CTT*	STU III	STICS	Goldwing	Cellular Phone	Courier
National Level		X					X	X			
Theater J2	X	X	X	X	X	A M	X	X			X
Corps Level	X	X	X	X	X	A M	X	X			
Country Team	X		X	X			X		X	X	X
Host Nation							X		X	X	X

*Note: A M (Alternate Means while aircraft is airborne)

Figure 12. IEW Architecture

Conclusion

The U.S. is likely to become more involved in LIC engagements during the next decade. This involvement may come as a result of humanitarian requirements, economic needs, or even requests for assistance from the United Nations or host-nations. Intelligence will be an important and necessary ingredient for successful policy formulation in any of these scenarios.

The intelligence community must take advantage of this "window of opportunity" to enhance the nation's intelligence capability to respond to LIC challenges. A key component of this intelligence capability is the tactical intelligence force structure. In order to achieve the desired results, this part of the force structure must be incorporated into the nation's overall intelligence effort in a manner never before witnessed during peacetime. The Unified Command J2 must exercise his authority with the intent of providing quality support to planning and operations by getting all intelligence elements involved in a complementary process and institutionalizing the "mindset transfer." This methodology affords both the tactical and strategic intelligence forces an opportunity to make positive contributions to the formulation of national LIC policy.

The adaptive process to modify conventional techniques must be documented to provide the junior analyst the much needed assistance to understand LIC-peculiar intelligence requirements by using conventional warfare intelligence procedures as the reference points to LIC understanding.

LIC scenarios must be exercised by all players in a BCTP-type "stress" environment. Intelligence support must be able to interact with the host-nation intelligence system prior to a crisis to work on techniques and procedures. The IEW architecture linkage to specific countries must be developed and validated early in the planning process in order of country priorities identified by the Unified Command J2 in regional assessments. This architecture must be routinely practiced with the goal of reducing processing and dissemination time to allow host-nations maximum time for flexibility in

developing options to counter the security challenges to their nation. If this is accomplished, the U.S. will stand a better chance of achieving success in LIC policy formulation and execution by virtue of quality intelligence support.

Notes

[1] *National Security Strategy of the United States*, p. 16.

[2] Joint Chiefs of Staff, *JCS Publication 3-07*, Doctrine for Joint operations in Low-Intensity Conflict, pp. 1,3,4. (hereafter referred to as *JCS Pub 3-07*).

[3] *Ibid.*

[4] U.S. Department of the Army, *Field Manual 100-20*, p. 1-1.

[5] *Ibid.*

[6] *Ibid.*

[7] *Ibid.*

[8] John Schlight, "Low-Intensity Conflict," *Army History*, No. 16, Fall 1990, p. 5.

[9] Alfred A. Smiley, "Intelligence Analysis in LIC," *Military Intelligence*, Vol. 16, No. 3, July/September 1990, p. 33.

[10] *JCS Pub 3-07*, p. I-9.

[11] *National Security Strategy of the United States*, p. 16.

[12] James B. Motley, "The Army's Need: A Relevant LIC Environment," *International Journal of Intelligence and Counterintelligence*, Vol. 4, No. 3, p. 395.

[13] John F. Stewart, BG, "Military Intelligence Operations in Low-Intensity Conflict: An Organizational Model," *Military Review*, Vol. LXVII, January 1988, p. 18.

[14] Smiley, p. 32.

[15] Motley, p. 391.

[16] *Ibid.*

[17] Paul E. Menohn, MG, "Vantage Point" *Military Intelligence*, Vol. 16, No. 3, July/September 1990, p. 2.

[18] Motley, p. 397.

[19] John H. Black, COL, "IEW Synchronization Matrix," *Military Intelligence*, Vol. 17, No. 4, October/December 1991, p. 32.

[20] David J. Rudock, CPT, "Getting the Razor's Edge on Collection Management," *Military Intelligence*, Vol. 17, No. 4, October/December 1991, p. 35.

[21] Black, p. 34.

[22] *Ibid.*, p. 33.

[23] Smiley, p. 32. Data base factors were developed from military intelligence analysis requirements.

[24] *Ibid.*, p. 34.

[25] Motley, p. 393.

[26] FM 100-20, p. Glossary 2. Country Team is the executive committee of an embassy, headed by the Chief of Mission and consisting of the principal representatives of the government departments and agencies present.

[27] *JCS Pub 3-07*, p. vii-1-2.

[28] *Ibid.*, p. vii-2.

[29] *Ibid.*

[30] *Ibid.*

[31] *Ibid.*

[32] *Ibid.*

[33] Michael H. Schoelwer, "The Failure of the U.S. Intelligence Community in Low-Intensity Conflict," *Low Intensity Conflict: The Pattern in the World*, p. 146. This is an ideal situation. Generally, decisions to commit and to leave are based on political pressures in the U.S.—not on dispassionate intelligence assessments.

[34] Stewart, p. 19.

[35] Carl W. Steiner, Witness Statement, House Appropriations Committee, Defense Subcommittee, 1991.

[36] Charles B. Eichelberger, LTG, "The MI Corps: A Vision of the Future," *Military Intelligence*, Vol. 17, No. 4, October/December 1991, p. 11.

[37] *Ibid.*

[38] *Ibid.*

[39] James A. Williams, LTG, "Intelligence, the Force Multiplier in Crisis," *Signal*, Vol. 38, No. 9, May 1984, p. 65.

[40] Stewart, p. 23.

Bibliography

Articles

Black, John H., COL. "IEW Synchronization Matrix." *Military Intelligence*, Vol. 17, No. 4, October/December 1991: 32-33.

Bigelow, Michael E., CPT. "A Historical Perspective on Low-Intensity Conflict: The Apache Campaigns under General Crook." *Military Intelligence*, Vol. 16, No. 3, July/September 1990: 38-41.

Eichelberger, Charles B., LTG (Retired). "The MI Corps: A Vision of the Future." *Military Intelligence*, Vol. 17, No. 4, October/December 1991: 7-13.

Linn, Brian M. "Intelligence and Low-Intensity Conflict in the Philippine War." *Intelligence and National Security*, Vol. 6, No. 1, January 1991: 90-114.

Menoher, Paul E., MG. "Vantage Point." *Military Intelligence*, Vol. 16, No. 3, July/September 1990: 2, 41.

Menoher, Paul E., MG. "Vantage Point." *Military Intelligence*, Vol. 18, No. 1, January/March 1992: 2, 41.

Metz, Steven. "US Strategy and the Changing LIC Threat." *Military Review*, Vol. LXXI, No. 6, June 1991: 22-29.

Motley, James B. "The Army's Need: A Relevant LIC Environment." *International Journal of Intelligence and Counterintelligence*, Vol. 4, No. 3: 383-405.

Rudock, David J. "Getting the Razor's Edge on Collection Management." *Military Intelligence*, Vol. 17, No. 4, October/December 1991: 32-34.

Schlight, John. "Low Intensity Conflict." *Army History*, PB 20-90-3, No. 16, Fall 1990: 5-6.

Schoelwer, Michael H. "The Failure of the U.S. Intelligence Community in Low-Intensity Conflict." *Low Intensity Conflict: The Pattern of Warfare in the Modern World.* Ed. Loren B. Thompson. Lexington Books, 1989.

Smiley, Alfred A., CPT. "Intelligence Analysis in LIC." *Military Intelligence.* Vol. 16, No. 3, July/September: 32-33.

Stewart, John F., BG. "Military Intelligence Operations in Low-Intensity Conflict: An Organizational Model." *Military Review*, Vol LXVII, January 1988: 17-27.

Ullmann, Don, COL. "HUNINT and the Operational Level of War." *Military Intelligence*, Vol. 18, No. 1, January/March 1991: 37-38.

Williams, James A., LTG, "Intelligence the Force Multiplier in Crisis." *Signal*, Vol. 38, No. 9, May 1984: 65-66.

Government Publications

Joint Chiefs of Staff. *JCS Publication 3-07: Doctrine for Joint Operations in Low-Intensity Conflict.* Washington: September 1990.

National Security Strategy of the United States. Washington: Government Printing Officer, August 1991.

U.S. Department of the Army. *Field Manual 24-12: Communications in a "Come-As-You-Are" War.* Washington: 17 July 1990.

U.S. Department of the Army. *Field Manual 34-2: Collection Management.* Washington: 20 October 1990.

U.S. Department of the Army. *Field Manual 34-60: Counterintelligence.* Washington: 5 February 1990.

U.S. Department of the Army. *Field Manual 34-36: Special Operations Forces Intelligence and Electronic Warfare Operations* (Final Draft). Washington: July 1990.

U.S. Department of the Army. *Field Manual 34-37: Echelons Above Corps (EAC) Intelligence and Electronic Warfare (IEW) Operations.* Washington: 15 January 1991.

U.S. Department of the Army. *Field Manual 34-80: Brigade and Battalion Intelligence and Electronic Warfare Operations.* Washington: 15 April 1986.

U.S. Department of the Army. *Field Manual 34-130: Intelligence Preparation of the Battlefield.* Washington: 23 May 1989.

U.S. Department of the Army. *Field Manual 100-5: Operations.* Washington: 5 May 1986.

U.S. Department of the Army. *Field Manual 100-20: Military Operations in Low-Intensity Conflict.* Washington: 1 December 1989.

Congressional Testimony

Steiner, Carl W., Gen. Witness Statement, House Appropriations Committee, Defense Subcommittee 1991.